Gröbner Bases and Invariant Theory

Wolfram Decker and Theo de Jong

FB 9 Mathematik, Universität des Saarlandes, Saarbrücken

"As all the roads lead to Rome so I find in my own case at least that all algebraic inquiries, sooner or later, end at the Capitol of modern algebra over whose shining portal is inscribed the Theory Of Invariants." (Sylvester (1864, p. 380))

"Like the Arabian phoenix rising out of its ashes, the theory of invariants, pronounced dead at the turn of the century, is once again at the forefront of mathematics. During its long eclipse, the language of modern algebra was developed, a sharp tool now at last being applied to the very purpose for which it was invented." (Kung *et al.* (1984))

0 Introduction

Historically, one root of invariant theory can be found in a problem of number theory, namely the problem of representing integers by quadratic binary forms

$$F = ax^2 + 2bxy + cy^2,$$

where a, b, c are integer coefficients. The discovery by Lagrange (1773, 1775) that such a representation is far from being unique lead to the notion of equivalence of quadratic binary forms. This was introduced in a rigorous way by Gauss (1801) in his Disquisitiones Arithmeticae. Gauss called two forms F and $\tilde{F}$ equivalent (properly equivalent) if F can be transformed into $\tilde{F}$ by a change of coordinates with determinant ± 1 $(+1)$. A key point is that the discriminant $(b^2 - ac)$ is invariant under such coordinate transformations (invariant functions in a, b, c are tools to distinguish between inequivalent forms). Indeed, in the situation of Gauss, if a change of coordinates

$$x \to \alpha x + \beta y, \quad y \to \gamma x + \delta y$$

transforms F into the form

$$\tilde{F} = \tilde{a}x^2 + 2\tilde{b}xy + \tilde{c}y^2,$$

then there is the relation

$$\tilde{b}^2 - \tilde{a}\tilde{c} = (b^2 - ac)(\alpha\delta - \beta\gamma)^2.$$

This relation is of course not only true in the modular context, we may allow complex coefficients as well. We therefore arrive at the following result which we state in the modern language of representation theory. The special linear group $\mathrm{SL}_2(\mathbb{C})$ acts on the vector space V of quadratic binary forms over $\mathbb{C}$ by linear substitution. The dual action on the space of coordinates a, b, c gives rise to an action of $\mathrm{SL}_2(\mathbb{C})$ on the symmetric algebra

$$\mathbb{C}[a,b,c] = \mathbb{C}[V] = S(V^*) = \bigoplus_{d \geq 0} S^d V^*,$$

that is, on the algebra of polynomial functions on V. The result is that the discriminant $\delta = b^2 - ac$ is an *invariant* under this action. Even more is true: every invariant can be written as a polynomial in δ (see for example Sturmfels (1993)). In other words, the graded *ring of invariants* $\mathbb{C}[V]^{\mathrm{SL}_2(\mathbb{C})}$ is generated as a $\mathbb{C}$–algebra by δ:

$$\mathbb{C}[V]^{\mathrm{SL}_2(\mathbb{C})} = \mathbb{C}[\delta].$$

Algebraic invariants such as the discriminant naturally show up in algebraic geometry, when one asks for properties of geometric objects, which are invariant under certain classes of transformations. For example, the geometric significance of the discriminant is that a quadratic binary form defines two distinct points on the projective line $\mathbb{P}^1(\mathbb{C})$ if and only if its discriminant is non–zero. People became interested in such invariant properties especially after the introduction of homogeneous coordinates by Möbius (1827) and Plücker (1830). This was a major impetus for invariant theory.

In the first decades of invariant theory, say between 1840 and 1870, people were mainly concerned with the discovery of particular invariants. The major case of interest was that of forms of degree d in n variables, d and n arbitrary, with $\mathrm{SL}_n(\mathbb{C})$ acting by linear substitution. One way of producing new invariants is to apply certain *covariants* (classically called *concomitants*) like the Hessian to an invariant already known. Cayley's Ω*–process* (compare Sturmfels (1993)) generates invariants more systematically by means of a differential operator. Another important tool for computing and presenting invariants is the *symbolic method* developed by Aronhold, Clebsch and Gordan (compare Dieudonné *et al.* (1971) , Kung *et al.* (1984), Sturmfels (1993)), and referred to as "the great war–horse of nineteenth century invariant theory" by Weyl, and as "Formelngestrüpp" or "Rechnerei" by E. Noether.

As time went on people realized that they could find in many explicit cases such as the example above a *fundamental system of invariants*, that is, a minimal finite system of homogeneous generators of the ring of invariants under consideration. The question whether there always exists a fundamental system of invariants is nowadays also known as *Hilbert's 14th problem* (Hilbert 1900). Gordan (1868) gave a positive answer to this question in the case of binary forms of any given degree. The proof, which is rather complicated, is based on the symbolic method. It is constructive and can in principle be used to compute fundamental systems of invariants (compare also Kung *et al.* (1984), Sturmfels (1993)).

Classical invariant theory culminated in Hilbert's two landmark papers (1890) and (1893). In these papers Hilbert introduced stunning new ideas which have deeply influenced the development of modern algebra and algebraic geometry. As an application of his ideas Hilbert proved a finiteness theorem for forms in n variables, n arbitrary.

The first paper contains a non-constructive proof of this result which relies on the *Basis Theorem*, proved in the same paper, and the Ω–process as a tool to generate invariants. Hilbert remarked that his proof actually applies in a wider range of cases, namely in those cases in which there exists an analogue to the Ω–process for the generation of invariants (compare also Weyl (1946, Appendix C)). Thus, in modern terminology, it applies to rational representations of linearly reductive groups. In particular, it applies to the *classical groups*, to *tori*, and to *finite groups* in the *non–modular case*, that is, in the case where the group order $|G|$ is invertible in the field of coefficients k. Hilbert also studied the successive relations (*syzygies*) between the elements $f_1, \ldots, f_r$ of a fundamental system of invariants. This chain of syzygies is of finite length $\leq r$ by Hilbert's *syzygy theorem* which is proved in the same paper. As a corollary of the syzygy theorem Hilbert proved the *Hilbert–Serre Theorem* on the structure of the *Hilbert function*.

In the second paper Hilbert gave a constructive proof for his finiteness result. This paper was Hilbert's quick answer to those of his fellow mathematicians who harshly criticized the non–constructiveness of his first proof. The second paper contains the *Nullstellensatz*, the *Hilbert–Mumford criterion* for *Null-forms*, and the *"Noether normalization theorem (graded case)"*.

Two of E. Noether's papers on invariant theory are concerned with the finiteness theorem for finite groups. In the first one (1916) she gave two short constructive proofs which also yield an explicit bound for the degree of the generators. In this paper Noether worked in characteristic zero but, under some assumptions on the group order, her ideas also apply to the case of characteristic p (compare for example Smith (1995)). The second paper (1926) settles the general case of arbitrary characteristic with a non–constructive proof.

Highlights of post–Hilbert invariant theory include Weyl's work on semi–simple groups in characteristic zero, Nagata's counterexample to Hilbert's 14th problem, Mumford's geometric invariant theory, and work of Nagata, Haboush and others, who proved the finiteness theorem for rational representations of *reductive groups* (compare Newstead (1978, pp. 90–92) for a short history of Hilbert's 14th problem and precise references). For an overview concerning degree bounds we refer to Derksen *et al.* (1995) .

Nowadays, with powerful computers available, one is tempted to come back to the explicit computation of invariants in interesting examples coming from algebraic geometry, invariant theory, physics, combinatorics (see Stanley (1979), or coding theory (see Sloane (1977)). The key point is, as demonstrated in Sturmfels' book (1993), that the classical computational techniques and Gröbner bases (Buchberger 1965, 1970, 1985, 1998) fit nicely together, and yield modern algorithms for invariant theory. In this context Gröbner bases are mainly used in order to compute syzygies and Hilbert functions, and for elimination (compare Eisenbud (1995) for an introduction to Gröbner bases). Another application of Gröbner bases is the computation of normalization (Vasconcelos 1991), (Gianni *et al.* 1996), (de Jong 1997), which is needed in Hilbert's algorithm (1893).

In this note we review some of the algorithms. We focus on recent developments which are not yet covered by Sturmfels (1993). We discuss variants of Kemper's algorithm for finite groups in arbitrary characteristic (Kemper 1996), and the remarkable discovery of Derksen (1997), that the ideas of Hilbert (1890) can be refined and turned into an algorithm.

Some of the algorithms presented here are already implemented, others are about to be implemented. We mention the Maple package Invar for finite groups by Kemper (1993), the Singular library finvar.lib for finite groups by Heydtmann (1997), and the package for finite groups coming with Magma (compare Kemper *et al.* (1997)).

1 Basic definitions and problems

Our basic setting consists of a group G, a field k, a vector space V over k of finite dimension n, and a representation $\rho : G \to \mathrm{GL}(V)$ of G on V. We suppose that coordinates $x_1, \ldots, x_n \in V^*$ are chosen. The action of G on V induces an action of G on V^*,

$$(\pi f)(v) = f(\rho(\pi^{-1})v),$$

and thus on

$$k[V] := k[x] := k[x_1, \ldots, x_n] := S(V^*) = \bigoplus_{d \geq 0} S^d V^*,$$

that is, on the graded k–algebra of polynomial functions on V (as usual be careful with this notion over finite fields). The basic objects of study in invariant theory are the fixed point sets of such actions.

Definition 1.1. The *ring of invariants* in the above setting is the graded subalgebra

$$k[V]^G := k[x]^G := \{f \in k[V] \mid \pi f = f \text{ for any } \pi \in G\} \subset k[V]. \quad \square$$

$k[V]^G$ only depends on the image $\rho(G) \subset \mathrm{GL}(V)$. We therefore may and will if necessary suppose that G is given as a subgroup of $\mathrm{GL}(V)$.

Definition 1.2. If $k[V]^G$ is finitely generated as a k–algebra then any minimal (that is irredundant) finite system $f_1, \ldots, f_r$ of homogeneous generators is called a *fundamental system of invariants.* □

If $k[V]^G$ is finitely generated over k then it is a Noetherian ring. Homogeneous elements $f_1, \ldots, f_r \in k[V]^G$ of positive degree generate $k[V]^G$ as a k–algebra if and only if they generate the ideal $k[V]^G_+ = \bigoplus_{d \geq 1} k[V]^G_d \subset k[V]^G$, or in turn if and only if the residue classes $\bar{f}_1, \ldots, \bar{f}_r$ generate $k[V]^G_+/(k[V]^G_+)^2$ as a vector space over k. This follows from Nakayama's Lemma. Thus the number of elements (and their degrees) in a fundamental system of invariants is uniquely determined as the embedding dimension of $k[V]^G$. The system itself however, is in general not uniquely determined.

Example 1.3. The symmetric group S_n acts on $k[x_1, \ldots, x_n]$ by permuting the coordinates. Elements of the corresponding ring of invariants $k[x]^{S_n}$ are called *symmetric polynomials.* Examples are the *elementary symmetric polynomials*

$$\begin{aligned} \sigma_1(x_1, \ldots, x_n) &:= x_1 + \ldots + x_n, \\ &\vdots \\ \sigma_n(x_1, \ldots, x_n) &:= x_1 \cdots x_n. \end{aligned}$$

It is well-known that every symmetric polynomial can be written as a polynomial in the elementary symmetric polynomials. In other words, $\sigma_1, \ldots, \sigma_n$ is a fundamental system of invariants. Even more is true: the expression of a symmetric polynomial in the elementary symmetric polynomials is unique since $\sigma_1, \ldots, \sigma_n$ are algebraically independent. Thus

$$k[x]^{S_n} = k[\sigma_1, \ldots, \sigma_n]$$

is a polynomial algebra. In characteristic zero, another system of algebraically independent generators of $k[x]^{S_n}$ over k is provided by the power sums

$$p_l(x_1, \ldots, x_n) = x_1^l + \cdots + x_n^l, \quad l = 1, \ldots, n. \quad \square$$

In general $k[V]^G$ is not a polynomial algebra. (Compare Mumford *et al.* (1994, Appendix to Chapter 4, A) for a discussion of classification results.) This means that in general we expect algebraic relations among the elements of a fundamental system of invariants. Thus we face two fundamental problems when studying a ring of invariants $k[V]^G$.

- **First fundamental problem of invariant theory**: Find a fundamental system of invariants $f_1, \ldots, f_r$ of $k[V]^G$.

- **Second fundamental problem of invariant theory**: Find the *syzygies* of $k[V]^G$.

The second problem means to find the successive relations between $f_1, \ldots, f_r$. To be more precise, let $z_1, \ldots, z_r$ be new variables, $\deg(z_i) = \deg(f_i)$, and consider the graded morphism

$$\phi_0 : k[z_1, \ldots, z_r] \to k[V]^G, \quad z_i \mapsto f_i.$$

Then the kernel I of ϕ_0 describes the algebraic relations between $f_1, \ldots, f_r$. I is finitely generated by Hilbert's basis theorem (1890). (Compare Gordan (1899), Cox *et al.* (1997) for a proof involving Gröbner bases.) There is an obvious but rather costly algorithm for the computation of I:

Remark 1.4. The algebraic relations between $f_1, \ldots, f_r$ can be computed as follows. Consider the ideal

$$\tilde{I} = (f_1 - z_1, \ldots, f_r - z_r) \subset k[x_1, \ldots, x_n, z_1, \ldots, z_r].$$

Choose an elimination order on $k[x_1, \ldots, x_n, z_1, \ldots, z_r]$ with respect to $x_1, \ldots, x_n$. Compute a Gröbner basis $\mathcal{G}$ of $\tilde{I}$ with respect to this order. Then the elements of $\mathcal{G}$ which do not involve $x_1, \ldots, x_n$ generate the elimination ideal

$$I = \tilde{I} \cap k[z_1, \ldots, z_r],$$

that is, the ideal of algebraic relations between $f_1, \ldots, f_r$.

Notice that an expression of a given element $f \in k[V]^G$ as a polynomial in $f_1, \ldots, f_r$ can be found by computing a normal form reduction modulo the Gröbner basis $\mathcal{G}$. □

A minimal set of homogeneous generators of I gives rise to a graded morphism $\phi_1 : F_1 \to k[z_1, \ldots, z_r]$ where F_1 is a free $k[z_1, \ldots, z_r]$–module of finite rank. By applying the same arguments to $\operatorname{Ker} \phi_1$ and so on we obtain the minimal free resolution

$$\cdots \to F_2 \xrightarrow{\phi_2} F_1 \xrightarrow{\phi_1} k[z_1, \ldots, z_r] \xrightarrow{\phi_0} k[V]^G \to 0$$

of $k[V]^G$ as a graded $k[z_1, \ldots, z_r]$–module. The elements of $\operatorname{Ker} \phi_{i-1}$ are the ith *order syzygies* on $k[V]^G$. Hilbert's syzygy theorem (1890), compare Schreyer (1980), Eisenbud (1995) for a proof involving Gröbner bases, tells us that all syzygies of order $\geq r + 1$ are zero.

Theorem 1.5 (Hilbert's Syzygy Theorem). *Let $k[z_1, \ldots, z_r]$ be a graded polynomial algebra and M a finitely generated graded $k[z_1, \ldots, z_r]$–module. Then the minimal free resolution of M is of type*

$$0 \to F_s \to \cdots \to F_1 \to F_0 \to M \to 0$$

for some $s \leq r$.

Applying for example Schreyer's variant of Buchberger's algorithm (Schreyer 1980), (Eisenbud 1995) for computing the syzygies of submodules of free modules over a polynomial algebra gives the higher order syzygies between $f_1, \ldots, f_r$.

Example 1.6. A beautiful interplay between geometry and invariant theory can be found in Klein's papers on modular curves. For example in Klein (1878/1879) he studies a natural embedding of the modular curve $X(7)$ of level 7 into the projective plane $\mathbb{P}^2(\mathbb{C})$. In fact, the embedded curve is defined by the quartic invariant

$$f = \lambda^3\mu + \mu^3\nu + \nu^3\lambda$$

of $G = \mathrm{PSL}_2(\mathbb{F}_7)$ acting on the homogeneous coordinate ring of $\mathbb{P}^2(\mathbb{C})$. G is a finite group of order 168, explicitly given as the subgroup of $\mathrm{GL}_3(\mathbb{C})$ generated by the matrices

$$\pi_1 = \begin{pmatrix} \gamma & 0 & 0 \\ 0 & \gamma^4 & 0 \\ 0 & 0 & \gamma^2 \end{pmatrix} \quad \text{and} \quad \pi_2 = \begin{pmatrix} A & B & C \\ B & C & A \\ C & A & B \end{pmatrix},$$

where $\gamma = e^{2\pi i/7}$ is a 7th root of unity, and where

$$A = \frac{(\gamma^5 - \gamma^2)}{\sqrt{-7}}, \quad B = \frac{(\gamma^3 - \gamma^4)}{\sqrt{-7}}, \quad C = \frac{(\gamma^6 - \gamma)}{\sqrt{-7}}.$$

From the single invariant f Klein successively derives further invariants by combining standard ad hoc techniques in invariant theory with geometric arguments. The second invariant he finds is the (suitably normalized) Hessian

$$\nabla = \frac{1}{54} \begin{vmatrix} \frac{\partial^2 f}{\partial\lambda^2} & \frac{\partial^2 f}{\partial\lambda\partial\mu} & \frac{\partial^2 f}{\partial\lambda\partial\nu} \\ \frac{\partial^2 f}{\partial\mu\partial\lambda} & \frac{\partial^2 f}{\partial\mu^2} & \frac{\partial^2 f}{\partial\mu\partial\nu} \\ \frac{\partial^2 f}{\partial\nu\partial\lambda} & \frac{\partial^2 f}{\partial\nu\partial\mu} & \frac{\partial^2 f}{\partial\nu^2} \end{vmatrix}$$

which has degree 6. The plane curves defined by ∇ and f intersect in the 24 flexes of the curve $\{f = 0\}$. Klein shows by using geometric arguments that the flexes form the only set of 24 points on $\{f = 0\}$ which is invariant under the action of G. Moreover, there is no such set of lower cardinality. Thus by Bezout's theorem f and ∇ are, up to scalars, the only invariants in degrees ≤ 6. Similar arguments show that the next possible degree for another generator of the invariant ring is 14 (recall that the curve $\{f = 0\}$ has 28 bitangents). Klein obtains an invariant of degree 14 which is different from $f^2\nabla$ by bordering the Hessian matrix:

$$C = \frac{1}{9} \begin{vmatrix} \frac{\partial^2 f}{\partial\lambda^2} & \frac{\partial^2 f}{\partial\lambda\partial\mu} & \frac{\partial^2 f}{\partial\lambda\partial\nu} & \frac{\partial\nabla}{\partial\lambda} \\ \frac{\partial^2 f}{\partial\mu\partial\lambda} & \frac{\partial^2 f}{\partial\mu^2} & \frac{\partial^2 f}{\partial\mu\partial\nu} & \frac{\partial\nabla}{\partial\mu} \\ \frac{\partial^2 f}{\partial\nu\partial\lambda} & \frac{\partial^2 f}{\partial\nu\partial\mu} & \frac{\partial^2 f}{\partial\nu^2} & \frac{\partial\nabla}{\partial\nu} \\ \frac{\partial\nabla}{\partial\lambda} & \frac{\partial\nabla}{\partial\mu} & \frac{\partial\nabla}{\partial\nu} & 0 \end{vmatrix}$$

Finally, he finds a fourth invariant by taking the Jacobian of f, ∇ and C:

$$K = \frac{1}{14}\begin{vmatrix} \frac{\partial f}{\partial \lambda} & \frac{\partial \nabla}{\partial \lambda} & \frac{\partial C}{\partial \lambda} \\ \frac{\partial f}{\partial \mu} & \frac{\partial \nabla}{\partial \mu} & \frac{\partial C}{\partial \mu} \\ \frac{\partial f}{\partial \nu} & \frac{\partial \nabla}{\partial \nu} & \frac{\partial C}{\partial \nu} \end{vmatrix}$$

Geometric arguments as above show that these four invariants generate the ring of invariants and that the relation

$$(-\nabla)^7 = (\frac{C}{12})^3 - 27(\frac{K}{216})^2.$$

generates the (first order) syzygies. □

Klein's arguments show that his ring of invariants is not a polynomial algebra. Finitely generated rings of invariants are, however, always integral over a polynomial algebra. This is due to a result of Hilbert (1893) which is nowadays known as the graded Noether normalization theorem (compare e.g. Bruns *et al.* (1993), Eisenbud (1995)). In the following all k–algebras will be associative, commutative, and with 1.

Theorem 1.7 (Graded Noether Normalization Theorem).
Let $A = \bigoplus_{d \geq 0} A_d$ be a finitely generated graded algebra over $A_0 = k$. Then there exist algebraically independent homogeneous elements $p_1, \ldots, p_m \in A$ such that A is integral over $k[p_1, \ldots, p_m]$.

It is a well–known fact that the number m does not depend on the particular Noether normalization. m is the *dimension* of A. Every system $p_1, \ldots, p_m$ as above is called a *homogeneous system of parameters.*

Theorem 1.8. *Let $A = \bigoplus_{d \geq 0} A_d$ be a finitely generated graded algebra of dimension m over $A_0 = k$.*

(1) The following are equivalent for homogeneous $p_1, \ldots, p_m \in A$:

  (a) $p_1, \ldots, p_m$ is a homogeneous system of parameters.
  (b) A is a finitely generated $k[p_1, \ldots, p_m]$–module.
  (c) $A/(p_1, \ldots, p_m)$ is a finite dimensional k–vector space.

(2) If A is an integral domain, then $m = \mathrm{trdeg}_k(A)$.

Here are two easy well–known criteria (compare e.g. Bruns *et al.* (1993)):

Lemma 1.9. *Let $A = \bigoplus_{d \geq 0} A_d$ be a finitely generated graded algebra over $A_0 = k$ of dimension m and $p_1, \ldots, p_i$ homogeneous elements of A. Then $\dim(A/(p_1, \ldots, p_i)) \geq m - i$ and equality holds if and only if $p_1, \ldots, p_i$ can be extended to a homogeneous system of parameters.*

Lemma 1.10. *Let $A = \bigoplus_{d\geq 0} A_d$ be a finitely generated graded algebra over $A_0 = k$ and let $p_1, \ldots, p_m$ be a homogeneous system of parameters. Then homogeneous $s_0, \ldots, s_l \in A$ form a minimal system of generators of A as a $k[p_1, \ldots, p_m]$–module if and only if the residue classes $\bar{s}_0, \ldots, \bar{s}_l$ form a basis of the k–vector space $A/(p_1, \ldots, p_m)$.*

Definition 1.11. If $A = k[V]^G$ is a finitely generated ring of invariants then any homogeneous system of parameters $p_1, \ldots, p_m$ is called a system of *primary invariants*. Any minimal system of homogeneous $s_0 = 1, s_1, \ldots, s_l$ generating $k[V]^G$ as a $k[p_1, \ldots, p_m]$–module is called a system of *secondary invariants*. □

Example 1.12. In 1.6 the invariants f, ∇, and C are algebraically independent. In particular, $\mathrm{trdeg}_{\mathbb{C}}\, \mathbb{C}[\lambda, \mu, \nu]^G = \mathrm{trdeg}_{\mathbb{C}}\, \mathbb{C}[\lambda, \mu, \nu] = 3$. In addition, Klein's geometric arguments show that f, ∇, and C cut out the empty subset of $\mathbb{P}^2(\mathbb{C})$. Therefore $\mathbb{C}[\lambda, \mu, \nu]/(f, \nabla, C)$ is a finite dimensional $\mathbb{C}$–vector space. So f, ∇, and C form a homogeneous system of parameters for $\mathbb{C}[\lambda, \mu, \nu]$ and thus also for $\mathbb{C}[\lambda, \mu, \nu]^G$. It is clear from the relation in 1.6 that 1 and K are corresponding secondary invariants. Of course, we could also take f, C, and K as primary invariants. Then $1, \nabla, \ldots, \nabla^6$ are corresponding secondary invariants. □

Primary and secondary invariants together (without $s_0 = 1$) provide a system of generators $f_1, \ldots, f_r$ of $k[V]^G$ as a k–algebra. But, as shown by the example, such a system might not be minimal. For each i one can check by linear algebra or via Gröbner bases whether f_i is contained in the $\deg(f_i)$–graded piece of the subalgebra generated by the remaining f_j. In this way superfluous generators can be detected and eliminated. Let us describe an alternative approach.

Remark 1.13. Suppose that

$$R := k[p_1, \ldots, p_m] \subset A = k[V]^G$$

is a Noether normalization. Let $s_0 = 1, s_1, \ldots, s_l$ be a minimal system of homogeneous generators of A as an R–module. Then one can describe A as a quotient of a polynomial ring in $m + l$ variables as follows. Let $y_1, \ldots, y_l$ be new variables, and consider the surjective map of k–algebras:

$$\psi : k[p_1, \ldots, p_m, y_1, \ldots, y_l] \longrightarrow A, \quad p_i \mapsto p_i,\ y_j \mapsto s_j.$$

The kernel of ψ describes the algebraic relations between the p_i and s_j. Let us single out two types of elements in $\operatorname{Ker}\psi$.

(1) Every R–module syzygy between the s_j, that is, every expression

$$\alpha_0 s_0 + \alpha_1 s_1 + \ldots + \alpha_l s_l = 0, \quad \alpha_i \in R,$$

gives an element $\alpha_0 + \alpha_1 y_1 + \ldots + \alpha_l y_l \in \operatorname{Ker}\psi$, which we call a *linear relation* .

(2) As A is also an R–algebra, one can form the products $s_i s_j$, $1 \leq i \leq j \leq l$. Since A is generated as an R–module by $s_0, \ldots, s_l$ there exist $\beta_{ijk} \in R$ such that $s_i s_j = \sum_k \beta_{ijk} s_k$. In this way we obtain $\binom{l+1}{2}$ elements $y_i y_j - \beta_{ij0} - \beta_{ij1} y_1 - \cdots - \beta_{ijl} y_l$ in $\operatorname{Ker} \psi$, which we call *quadratic relations.*

It is an easy fact that the kernel of ψ is generated by the linear and the quadratic relations. Superfluous generators among $p_1, \ldots, p_m, s_1, \ldots, s_l$ correspond to terms in these relations which are linear in either one of the p_i or one of the s_j. By eliminating these generators and the corresponding relations we eventually arrive at a fundamental system of invariants, and the remaining linear and quadratic relations generate the first order syzygies between these fundamental invariants. □

In those cases where A is a free R–module there are no linear relations. This property can be taken as a definition for A to be Cohen–Macaulay (compare Bruns *et al.* (1993), Springer (1989)):

Definition 1.14. Let $A = \bigoplus_{d \geq 0} A_d$ be a finitely generated graded algebra of dimension m over $A_0 = k$. Then A is *Cohen–Macaulay* if for some (and hence for any) homogeneous system of parameters $p_1, \ldots, p_m$ A is a free $k[p_1, \ldots, p_m]$–module. □

Rings of invariants are Cohen–Macaulay in a wide range of cases (compare the following section). In these cases one only has to compute the quadratic relations. This can be done by linear algebra or via Gröbner bases. Knowing the β_{ijk} one can write down a not necessarily minimal free resolution of $\operatorname{Ker} \psi$ as a $k[p_1, \ldots, p_m, y_1, \ldots, y_l]$–module without computing syzygies (Eisenbud *et al.* 1981).

For later use we recall some results on Hilbert functions. For details and proofs we refer to Bruns *et al.* (1993), Smith (1995) .

Definition 1.15. Let $A = \bigoplus_{d \geq 0} A_d$ be a finitely generated graded algebra over $A_0 = k$. The function

$$H(A, \_) : \mathbb{N} \to \mathbb{N}, \quad d \to \dim_k A_d$$

is the *Hilbert function* of A, and

$$H_A(t) = \sum_{d \geq 0} H(A, d) t^d$$

is the *Hilbert series* of A. □

Remark 1.16.

(1) If $A = k[f_1, \ldots, f_r]$ is a polynomial algebra, then the Hilbert series of A is of the form

$$H_A(t) = \frac{1}{\prod_{i=1}^{r} (1 - t^{\deg(f_i)})}.$$

(2) If A is Cohen–Macaulay, $p_1, \ldots, p_m$ form a homogeneous system of parameters, and $s_0, \ldots, s_l$ is a basis of A as a free $k[p_1, \ldots, p_m]$–module, then

$$H_A(t) = \frac{\sum_{j=0}^{l} t^{\deg(s_j)}}{\prod_{i=1}^{m}(1 - t^{\deg(p_i)})}. \qquad \square$$

Example 1.17. In 1.6, 1.12 the Hilbert series is

$$H_{\mathbb{C}[\lambda,\mu,\nu]^G}(t) = \frac{1 + t^{21}}{(1-t)^4(1-t)^6(1-t)^{14}} = \frac{1 + t^6 + t^{12} + \ldots t^{36}}{(1-t)^4(1-t)^{14}(1-t)^{21}}$$

$$= 1 + t^4 + t^6 + t^8 + t^{10} + 2t^{12} + 2t^{14} + 2t^{16} + 3t^{18} + 3t^{20} + t^{21} + \ldots. \qquad \square$$

The additivity of the Hilbert function, Hilbert's syzygy theorem, and Remark 1.16, (1) yield the following

Theorem 1.18 (Hilbert–Serre). *Let $A = \bigoplus_{d \geq 0} A_d$ be a graded algebra which is finitely generated over $A_0 = k$ by homogeneous elements $f_1, \ldots, f_r$ of positive degrees. Then the Hilbert series of A is of the form*

$$H_A(t) = \frac{p(t)}{\prod_{i=1}^{r}(1 - t^{\deg(f_i)})}$$

for some $p(t) \in \mathbb{Z}[t]$.

2 Algorithms for finite groups

We start with E. Noether's finiteness theorem (Noether 1926). The non–constructive proof, which is in principle Noether's original proof, is taken from Smith (1995).

Theorem 2.1 (Noether's Finiteness Theorem). *Let $\rho : G \to \mathrm{GL}(V)$ be a representation of a finite group G on the n–dimensional k–vector space V. Then $k[V]$ is integral over $k[V]^G$. In particular,*

$$\mathrm{trdeg}_k\, k[V]^G = \mathrm{trdeg}_k\, k[V] = n.$$

Moreover, $k[V]^G$ is finitely generated as a k–algebra.

Proof. Let $f \in k[V] = k[x_1, \ldots, x_n]$. Then f is a root of the monic univariate polynomial

$$P_f(t) := \prod_{\pi \in G}(t - \pi f) \in k[V][t].$$

The coefficients of P_f belong to $k[V]^G$ since they are elementary symmetric polynomials in the elements πf, $\pi \in G$. It follows that $k[V]$ is integral over $k[V]^G$. In particular, $\operatorname{trdeg}_k k[V]^G = \operatorname{trdeg}_k k[V] = n$.

Let A be the subalgebra of $k[V]^G$ generated by the coefficients of the monic polynomials $P_{x_1}, \ldots, P_{x_n}$. Then $k[V]$ is integral over A as well, and hence $k[V]$ is finitely generated as an A–module. Since A is Noetherian also the submodule $k[V]^G$ of $k[V]$ is finitely generated as an A–module. It follows that $k[V]^G$ is finitely generated as a k–algebra. □

Next we introduce an important tool for the invariant theory of a finite group G. This tool is defined if the characteristic of k is zero, or a prime number which does not divide the group order $|G|$.

Remark and Definition 2.2. Let G be a finite group such that $|G|$ is invertible in k. Then

$$R : k[V] \to k[V], \quad f(x) \mapsto \frac{1}{|G|} \sum_{\pi \in G} (\pi f)(x)$$

is a well–defined k–linear graded map which projects $k[V]$ onto $k[V]^G$. Moreover, R is a $k[V]^G$–module homomorphism. R is called *Reynolds operator.* □

The following result first appeared in Hochster *et al.* (1971), but had been known before. The proof we present is taken from Stanley (1979).

Theorem 2.3. *Let G be a finite group such that $|G|$ is invertible in k. Then $k[V]^G$ is Cohen–Macaulay.*

Proof. Let

$$k[p_1, \ldots, p_n] \subset k[V]^G$$

be a Noether normalization. Since $k[V]$ is integral over $k[V]^G$ by Theorem 2.1, it is also integral over $k[p_1, \ldots, p_n]$. Therefore $p_1, \ldots, p_n$ is also a homogeneous system of parameters for $k[V]$. As $k[V]$ is Cohen–Macaulay, it follows that $k[V]$ is a free $k[p_1, \ldots, p_n]$–module. By Lemma 1.10 homogeneous $s_0, \ldots, s_r$ generate $k[V]$ as a $k[p_1, \ldots, p_n]$–module if and only if their residue classes generate $k[V]/(p_1, \ldots, p_n)$ as a k–vector space.
Now notice that $k[V] = k[V]^G \oplus \operatorname{Ker} R$ is a decomposition into $k[V]^G$–modules by 2.2. Choose homogeneous $s_0, \ldots, s_l \in k[V]^G$ and $s_{l+1}, \ldots, s_r \in \operatorname{Ker} R$ such that $\bar{s}_0, \ldots, \bar{s}_l$ and $\bar{s}_{l+1}, \ldots, \bar{s}_r$ are k–bases of $k[V]^G/(p_1, \ldots, p_n)$ and $\operatorname{Ker} R / \sum_{i=1}^n p_i \operatorname{Ker} R$ resp. This gives a decomposition

$$k[V]^G = \bigoplus_{j=0}^{l} s_j k[p_1, \ldots, p_n],$$

hence $k[V]^G$ is Cohen–Macaulay. □

This theorem holds more generally for rational representations of linearly reductive groups (see Hochster *et al.* (1974)).

Definition 2.4. Let G be a finite group. We speak of *non–modular* invariant theory if $|G|$ is invertible in k, and of *modular* invariant theory otherwise. $\square$

In the following G will be a finite group explicitly given as a matrix group $G \subset \mathrm{GL}_k(V^*) \cong \mathrm{GL}_n(k)$ by a finite set of generating matrices, and acting on $k[V] \cong k[x]$ by linear substitution: $\pi f(x_1, \dots, x_n) = f((x_1, \dots, x_n) \cdot \pi)$.

How to compute a fundamental system of invariants? As in Klein's Example 1.6 the basic strategy is to proceed degree by degree. Thus the first task is to calculate for a given degree d a k–basis of the graded piece $k[x]_d^G$. There are two basic methods. To be invariant under just one element of G imposes a linear condition on the homogeneous polynomials of a given degree d. Therefore, for each d, we may compute a k–basis of $k[x]_d^G$ by solving a linear system of equations which depends on the given set of generators of G. In the non–modular case we may evaluate the Reynold's operator R in the monomials of degree d in order to calculate a k–basis of $k[x]_d^G$. If a priori information on the dimension of $k[x]_d^G$ is available we can stop evaluating R as soon as the right number of invariants has been computed. Therefore already at this point, it is useful to precompute the Hilbert series of $k[x]^G$. This is possible due to a result of Molien (1897) (compare Heydtmann (1996)).

Theorem 2.5 (Molien's Theorem). *In the non–modular case the Hilbert series of $k[x]^G$ is given as the Molien series of G which is defined as follows.*

(1) Let $\operatorname{char} k = 0$. *Then the Molien series of G is*

$$\frac{1}{|G|} \sum_{\pi \in G} \frac{1}{\det(1 - t\pi)}.$$

(2) Let $\operatorname{char} k = p > 0$, *$|G|$ not divisible by p. Fix primitive $|G|$th roots of unity over k and $\mathbb{Q}$ resp., say λ and $\tilde{\lambda}$. For $\pi \in G$ let $\lambda^{k_1(\pi)}, \dots, \lambda^{k_n(\pi)}$ be the eigenvalues of π and*

$$\Phi_\pi(t) = \prod_{i=1}^{n} (1 - t\tilde{\lambda}^{k_i(\pi)}).$$

Then the Molien series of G is

$$\frac{1}{|G|} \sum_{\pi \in G} \frac{1}{\Phi_\pi(t)}.$$

Summing up what we have so far gives a first algorithm in the non–modular case: Compute invariants degree by degree until the Hilbert series of the k–subalgebra of $k[x]^G$ generated by the invariants computed so far equals the

Molien series. Or, again in the non–modular case, use degree bounds such as Noether's degree bound (1916) or that of Campbell *et al.* (1991) as criteria for termination.

Another idea, which yields more effective algorithms, is to compute a Noether normalization of $k[x]^G$ first. In the case of finite groups, by Theorem 2.1, every homogeneous system of parameters for $k[x]^G$ contains precisely n elements, and $p_1, \ldots, p_n \in k[x]^G$ are a homogeneous system of parameters for $k[x]^G$ if and only if they are a homogeneous system of parameters for $k[x]$. Lemma 1.9 suggests how to compute such a system $p_1, \ldots, p_n$ successively. If $p_1, \ldots, p_i$ with $\dim((p_1, \ldots, p_i)) = n-i$ are already constructed, then we need to find a homogeneous invariant q such that $\dim((p_1, \ldots, p_i, q)) = n-i-1$. Refining this idea yields the

Algorithm 2.6 (Primary invariants). (Decker *et al.* 1997)

Input: Generators of G.

Output: Primary invariants for $k[x]^G$.

Procedure:

Initialize $d := i := 0$.
repeat
  Set $d := d + 1$.
  Compute a basis $b_1, \ldots, b_{c_d}$ of $k[x_1, \ldots, x_n]^G_d$.
  Compute $m = \dim((p_1, \ldots, p_i, b_1, \ldots, b_{c_d}))$ via Gröbner bases.
  while $n - i > m$ **do**
    if k infinite **then**
      set $i := i + 1$.
      Find a k–linear combination p_i of $b_1, \ldots, b_{c_d}$ such that
        $\dim((p_1, \ldots, p_{i-1})) > \dim((p_1, \ldots, p_i))$.
    else
      find a new k–linear combination q of $b_1, \ldots, b_{c_d}$.
      if $\dim((p_1, \ldots, p_i)) > \dim((p_1, \ldots, p_i, q)$ **then**
        set $i := i + 1$, $p_i := q$.
      if all linear combinations of $b_1, \ldots, b_{c_d}$ have been tested **then**
        break [of **while**–loop]
  end [of **while**–loop]
until $i = n$
return: $p_1, \ldots, p_n$
end [of **Procedure**].

From now on suppose that a system of primary invariants $p_1, \ldots, p_n$ and a Gröbner basis $\mathcal{G}$ of the ideal $(p_1, \ldots, p_n)$ are already given. The next step is to compute a system of secondary invariants, that is, a minimal system of homogeneous generators of $k[x]^G$ as a $k[p_1, \ldots, p_n]$–module.

We first deal with the non–modular case. In this case the Reynolds operator R is available. By 2.2 R is a homomorphism of $k[x]^G$–modules and thus also of $k[p_1, \ldots, p_n]$–modules. Hence homogeneous generators of $k[x]^G$ as a $k[p_1, \ldots, p_n]$–module can be obtained by applying R to a (minimal) system of homogeneous generators of $k[x]$ as a $k[p_1, \ldots, p_n]$–module, that is, to a system of homogeneous polynomials whose residue classes are a basis of the k–vector space $k[x]/(p_1, \ldots, p_n)$ (compare Lemma 1.10). We may thus apply R to the finitely many monomials which are not in the initial ideal of $(p_1, \ldots, p_n)$ (with respect to the chosen monomial order). In this way we obtain a not necessarily minimal system of generators of $k[x]^G$ as a $k[p_1, \ldots, p_n]$–module. In order to avoid superfluous computations we refine the algorithm as follows. Write $(p_1, \ldots, p_n)^{k[x]^G}$ for the ideal generated by $p_1, \ldots, p_n$ in $k[x]^G$. Again by Lemma 1.10 homogeneous $s_0, \ldots, s_j \in k[x]^G$ can be extended to a system of secondary invariants if and only if their residue classes modulo $(p_1, \ldots, p_n)^{k[x]^G}$ are linearly independent. This in turn is equivalent to the fact that $s_0, \ldots, s_j$ are linearly independent modulo $(p_1, \ldots, p_n)$ (apply 2.2 to show that the natural map $k[x]^G/(p_1, \ldots, p_n)^{k[x]^G} \to k[x]/(p_1, \ldots, p_n)$ is injective). Since everything is homogeneous it is enough to check that for every d the normal forms with respect to $\mathcal{G}$ of those s_i having degree d are linearly independent. This check can be performed by solving a linear system of equations, or by a Gröbner basis calculation. The following numerical information provides a criterion for termination.

Remark 2.7. Let $|G|$ be invertible in k. Then $k[x]^G$ is Cohen–Macaulay, and we may compute the Hilbert series of $k[x]^G$ in two different ways. Comparing the formulae in 1.16, (2) and 2.5 gives the following result (see e.g. Heydtmann (1996)):

(1) The degrees d_j of the secondary invariants and their number k_j in each degree resp. are uniquely determined as the exponents and the coefficients resp. of the univariate polynomial

$$\sum_{j=0}^{b} m_j t^{d_j} := H_{K[x]^G}(t) \prod_{i=1}^{n} (1 - t^{\deg(p_i)}).$$

(2) The total number of secondary invariants equals

$$\frac{1}{|G|} \prod_{i=1}^{n} \deg(p_i). \qquad \square$$

Example 2.8. (1) In 1.6, 1.12, with primary invariants f, ∇ and C, the polynomial in 2.7, (1) reads

$$H_{\mathbb{C}[\lambda,\mu,\nu]^G}(t)(1 - t^4)(1 - t^6)(1 - t^{14}) = 1 + t^{21}.$$

With primary invariants f, C and K we obtain

$$H_{\mathbb{C}[\lambda,\mu,\nu]^G}(t)(1-t)^4(1-t)^{14}(1-t)^{21} = 1 + t^6 + t^{12} + \cdots + t^{36}.$$

(2) The Heisenberg group H_5 of level 5 in its Schrödinger representation is the subgroup of $\mathrm{GL}_5(\mathbb{C})$ generated by the matrices

$$\pi_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad \pi_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \xi & 0 & 0 & 0 \\ 0 & 0 & \xi^2 & 0 & 0 \\ 0 & 0 & 0 & \xi^3 & 0 \\ 0 & 0 & 0 & 0 & \xi^4 \end{pmatrix},$$

where $\xi = e^{2\pi i/5}$ is a 5th root of unity. H_5 is a finite group of order 125. A partial expansion of the Molien series is

$$1 + 6t^5 + 41t^{10} + 156t^{15} + 426t^{20} + 951t^{25} + 1856t^{30} + \dots \quad .$$

The invariants in degree 5 are the Horrocks–Mumford quintics (Horrocks *et al.* 1973). The Algorithm 2.6 finds three primary invariants in degree 5, and two in degree 10. The corresponding polynomial as in 2.7, (1) reads

$$1 + 3t^5 + 24t^{10} + 44t^{15} + 24t^{20} + 3t^{25} + t^{30}.$$

Thus, including 1, there are 100 secondary invariants of degrees up to 30. See Heydtmann (1996), where this example is worked out with the help of finvar.lib (Heydtmann 1997).

(3) The modular curve $X(11)$ is studied in Klein (1879). Klein discovered that X(11) is the singular locus of the cubic threefold in $\mathbb{P}^4(\mathbb{C})$ defined by

$$\nabla = y_1^2 y_9 + y_4^2 y_3 + y_5^2 y_1 + y_9^2 y_4 + y_3^2 y_5,$$

where y_1, y_4, y_5, y_9, y_3 are the homogeneous coordinates of $\mathbb{P}^4(\mathbb{C})$. ∇ is a cubic invariant of $G = \mathrm{PSL}_2(\mathbb{F}_{11})$ acting on the homogeneous coordinate ring of $\mathbb{P}^4(\mathbb{C})$. Explicitly, G is the subgroup of $\mathrm{GL}_5(\mathbb{C})$ generated by the matrices

$$\pi_1 = \begin{pmatrix} \rho & 0 & 0 & 0 & 0 \\ 0 & \rho^4 & 0 & 0 & 0 \\ 0 & 0 & \rho^5 & 0 & 0 \\ 0 & 0 & 0 & \rho^9 & 0 \\ 0 & 0 & 0 & 0 & \rho^3 \end{pmatrix} \quad \text{and} \quad \pi_2 = \begin{pmatrix} A & B & C & D & E \\ B & C & D & E & A \\ C & D & E & A & B \\ D & E & A & B & C \\ E & A & B & C & D \end{pmatrix},$$

where $\rho = e^{2\pi i/11}$ is a 11th root of unity, and where

$$A = \frac{(\rho^9 - \rho^2)}{\sqrt{-11}}, \quad B = \frac{(\rho^4 - \rho^7)}{\sqrt{-11}}, \quad C = \frac{(\rho^3 - \rho^8)}{\sqrt{-11}},$$

$$D = \frac{(\rho^5 - \rho^6)}{\sqrt{-11}}, \quad E = \frac{(\rho - \rho^{10})}{\sqrt{-11}}.$$

G is a finite group of order 660. Besides ∇ Klein only needs two more invariants for his purposes. One of them is the (suitably normalized) Hessian of ∇,

$$H = \begin{vmatrix} y_9 & 0 & y_5 & y_1 & 0 \\ 0 & y_3 & 0 & y_9 & y_4 \\ y_5 & 0 & y_1 & 0 & y_3 \\ y_1 & y_9 & 0 & y_4 & 0 \\ 0 & y_4 & y_3 & 0 & y_5 \end{vmatrix}.$$

A complete description of $\mathbb{C}[y]^G$ is given by Adler (1992) along the following lines. Adler starts his paper by quoting Klein (1879):

"Es ist nicht meine Absicht, alle ungeändert bleibenden ganzen Funktionen der y mitzuteilen; dies würde jedenfalls eine weitläufige und vielleicht eine schwierige Aufgabe sein."

The Molien series of $\mathbb{C}[y]^G$ is known to Adler from a letter of Edge:

$$H_{\mathbb{C}[y]^G}(t) = \frac{1 + t^7 + t^9 + t^{10} + t^{12} + 2t^{14} + t^{16} + t^{18} + t^{19} + t^{21} + t^{28}}{(1-t^3)(1-t^5)(1-t^6)(1-t^8)(1-t^{11})}$$

$$= 1 + t^3 + t^5 + 2t^6 + t^7 + 2t^8 + 3t^9 + 3t^{10} + 4t^{11} + \dots \quad .$$

Comparing with 2.7 one can hope to find primary invariants of degrees 3, 5, 6, 8, and 11 resp., and secondary invariants in the degrees prescribed by the numerator polynomial. Let us follow Adler's notation and provide every invariant with a subscript indicating the degree. Starting with the two invariants $f_3 := \nabla$ and $f_5 := H$, Adler derives two systems of invariants,

$$\mathcal{P} = \{f_3, f_5, f_6, f_8, f_{11}\},$$

and

$$\mathcal{S} = \{1, f_7, f_9, f_{10}, f_{12}, f_{14}, f_7^2, f_7 f_9, f_9^2, f_9 f_{10}, f_7^3, f_9^2 f_{10}\},$$

in the spirit of classical invariant theory. To be more precise, if $\Phi \in \mathbb{C}[y]^G$ is given, then define the differential operator D_Φ by

$$D_\Phi = \Phi(\frac{\partial}{\partial y_1}, \frac{\partial}{\partial y_4}, \frac{\partial}{\partial y_5}, \frac{\partial}{\partial y_9}, \frac{\partial}{\partial y_3}).$$

Then $D_\Phi(\Psi) \in \mathbb{C}[y]^G$ for every $\Psi \in \mathbb{C}[y]^G$. With $D = D_{f_3}$ Adler obtains e.g. the invariants

$$f_6 = \frac{1}{12}(D(f_3^3 - 168 f_3^2), \quad f_8 = \frac{1}{4}(D(f_3^2 f_5) - 150 f_3 f_5),$$

and

$$f_{11} = \frac{1}{2} D(f_3^2 f_8) - 219 f_3^2 f_5 + 56 f_5 f_6 - 150 f_3 f_8$$

(see Adler (1992) for $f_7, f_9, f_{10}, f_{12}, f_{14}$). Adler checks that the Jacobian matrix of the invariants in $\mathcal{P}$ does not vanish identically. Therefore these invariants are algebraically independent over $\mathbb{C}$. Now Adler proves by more or less explicit computations involving the quadratic relations as in 1.13 that $R_0 = \mathbb{Q}[f_3, f_5, f_6, f_8, f_{11}, f_7, f_9, f_{10}, f_{12}, f_{14}]$ is a free $A_0 = \mathbb{Q}[f_3, f_5, f_6, f_8, f_{11}]$–module with basis $\mathcal{S}$. The next step is to show that $R_0 \otimes \mathbb{C} \cong \mathbb{C}[y]^G$. This is a check on Hilbert functions. Altogether it follows that the elements of $\mathcal{P}$ are a homogeneous system of parameters, that $\mathbb{C}[y]^G$ is a free $\mathbb{C}[\mathcal{P}]$–module with basis $\mathcal{S}$, and that $f_3, f_5, f_6, f_7, f_8, f_9, f_{10}, f_{11}, f_{12}, f_{14}$ is a fundamental system of invariants with fifteen relations. □

The following algorithm singles out those secondary invariants which are not products of powers of secondary invariants of lower degree. Following Kemper *et al.* (1997) we call these secondary invariants *irreducible* (and the others, including 1, *reducible*). We write $\mathrm{NF}(f)$ for the normal form of a polynomial $f \in k[x]$ with respect to the fixed Gröbner basis $\mathcal{G}$.

Algorithm 2.9 (Secondary invariants in the non–modular case). (Kemper *et al.* 1997)

Input: Reynolds operator R, Hilbert series $H_{k[x]^G}(t)$, primary invariants $p_1, \ldots, p_n$ for $k[x]^G$, a Gröbner basis $\mathcal{G}$ of $(p_1, \ldots, p_n)$.

Output: Secondary invariants for $k[x]^G$ (irreducible and reducible).

Procedure:

Compute the polynomial $\sum_{j=0}^{b} m_j t^{d_j} = H_{K[x]^G}(t) \prod_{i=1}^{n} (1 - t^{\deg(p_i)})$.
Initialize $I := \emptyset,\ P := \{1\}$.
for $j = 1, \ldots, b$ **do**
  set i:=0.
  while $i < m_j$ **do**
    for all power products q of elements of I having degree d_j **do**
      if $\mathrm{NF}(s_1), \ldots, \mathrm{NF}(s_i), \mathrm{NF}(q)$ are linearly independent
          modulo $(p_1, \ldots, p_n)$ **then**
        set $i := i + 1,\ s_i := q,\ P := P \cup \{s_i\}$.
    end [of **for**–loop]
    Compute the monomials $m_1, \ldots, m_c$ of degree d_j which are
      not in the initial ideal of $(p_1, \ldots, p_n)$
    for $r = 1, \ldots, c$ **do**
      if $\mathrm{NF}(s_1), \ldots, \mathrm{NF}(s_i), \mathrm{NF}(R(m_r))$ are linearly independent
          modulo $(p_1, \ldots, p_n)$ **then**
        set $i := i + 1,\ s_i := R(m_r),\ I := I \cup \{s_i\}$.
    end [of **for**–loop]
  end [of **while**–loop]

end [of **for**–loop]
return: I, P
end [of **Procedure**].

It is easy to see that for the calculation of fundamental invariants and syzygies as in Remark 1.13 it is enough to check the products of type $s_i s_j$, $s_i \in I$ and $s_j \in I \cup (P \setminus \{1\})$.

Remark 2.10. The computation of secondary invariants in the modular case can be reduced to the computation of secondary invariants in the non–modular case by an idea of Kemper (1996) (compare also Kemper *et al.* (1997)). Choose a subgroup $H \subset G$ such that $|H|$ is invertible in k (for example, the trivial subgroup will do). The given primary invariants $p_1, \ldots, p_n$ for G are also primary invariants for H. Write $A = k[p_1, \ldots, p_n]$. Compute secondary invariants $t_1, \ldots, t_m$ for H with respect to $p_1, \ldots, p_n$ (for example by Algorithm 2.9). Choose a subset $\Delta \subset G$ such that the elements of $\Delta \cup H$ generate G. Then there is a commutative diagram of graded $k[p_1, \ldots, p_n]$–modules with exact rows and columns,

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \uparrow & & \uparrow & & \uparrow \\
0 & \longrightarrow & k[x]^G & \rightarrow & k[x]^H & \xrightarrow{\alpha} & \bigoplus_{\pi \in \Delta} k[x] \\
 & & \uparrow & & \beta \uparrow & & \uparrow \\
0 & \rightarrow & M & \longrightarrow & A^m & \xrightarrow{\tilde{\alpha}} & A^r \\
 & & \uparrow & & \uparrow & & \uparrow \\
 & & 0 & & 0 & & 0
\end{array}$$

where α is defined by $f \mapsto (\pi f - f)_{\pi \in \Delta}$, β is the map $(f_1, \ldots, f_m) \mapsto \sum_{j=1}^m f_j t_j$, and $r = |\Delta| \cdot \prod_{i=1}^n \deg(p_i)$. Indeed, $k[x]$ is a free $k[p_1, \ldots, p_n]$–module of rank $\prod_{i=1}^n \deg(p_i)$ with a basis $\mathcal{B}$ given by those monomials which are not in the initial ideal of $(p_1, \ldots, p_n)$ (with respect to the chosen monomial order). The map $\tilde{\alpha}$, that is, the representation of each $(\pi t_j - t_j)$ in terms of $\mathcal{B}$, can be computed by linear algebra or via Gröbner bases. In this way the computation of secondary invariants for G and of the $k[p_1, \ldots, p_n]$–module relations between the secondary invariants can be reduced to the computation of syzygies of submodules of free $k[p_1, \ldots, p_n]$–modules. $\square$

Example 2.11. Kemper (1996) applies his algorithm to an example of Bertin (1967). The cyclic group G of order 4 acts on $\mathbb{F}_2[x_1, \ldots, x_4]$ by cyclic permutations of the variables. Kemper finds the primary invariants

$$p_1 = x_1 + x_2 + x_3 + x_4, \quad p_2 = x_1x_3 + x_2x_4,$$

$$p_3 = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1, \quad p_4 = x_1x_2x_3x_4.$$

Choose the trivial subgroup H of G. The corresponding polynomial as in 2.7, (1) reads $1 + 3t + 4t^2 + 4t^3 + 3t^4 + t^5$. From the 16 secondary invariants for H Kemper obtains 5 secondary invariants for G,

$$s_0 = 1, s_1 = x_1^3 + x_2^3 + x_3^3 + x_4^3, \quad s_2 = x_1^2x_2 + x_2^2x_3 + x_3^2x_4 + x_4^2x_1,$$

$$s_3 = x_1^3x_2 + x_2^3x_3 + x_3^3x_4 + x_4^3x_1, \quad s_4 = x_1^3x_2^2 + x_2^3x_3^2 + x_3^3x_4^2 + x_4^3x_1^2,$$

and the relation

$$p_1(p_1^4 + p_2^2 + p_2p_3)s_1 + (p_1^2 + p_2 + p_3)s_2 + (p_1^2 + p_2)s_3 + p_1s_4 = 0.$$

It follows that $\mathbb{F}_2[x]^G$ is not Cohen–Macaulay. □

Remark 2.12.

(1) The following is easy to see (compare Kemper (1996)): let $p_1, \ldots, p_n$ be a system of primary invariants of degrees $d_1, \ldots, d_n$. Then $k[x]^G$ is Cohen–Macaulay if and only the number of secondary invariants equals $(\prod_{i=1}^n d_i)/|G|$.

(2) A check on the algorithms for secondary invariants shows that it is crucial to start with primary invariants $p_1, \ldots, p_n$ such that the product $\prod_{i=1}^n \deg(p_i)$ is as small as possible. Algorithm 2.6 does not always produce primary invariants with $\prod_{i=1}^n \deg(p_i)$ minimal. See Kemper (1997) for examples and a solution to this problem.

(3) For Adler's bicycles, which grew out of an attempt "to understand from a general point of view the results of Felix Klein on the equations defining modular curves of prime order" we refer to Adler (1997). □

3 Algorithms for linearly reductive groups

In this section our field of coefficients is $k = \mathbb{C}$, if not explicitly stated otherwise.

First we recall the notion of a linearly reductive group. The general linear group $\mathrm{GL}_m(k)$ is the Zariski open subset of k^{m^2} defined by $\det(x_{ij}) \neq 0$. We may identify $\mathrm{GL}_m(k)$ with the Zariski closed subset of k^{m^2+1} defined by the polynomial equation $z \cdot \det(x_{ij}) = 1$, where z is an additional coordinate. Thus $\mathrm{GL}_m(k)$ is an affine variety with coordinate ring

$$k[GL_m(k)] \cong k[x_{ij}, \det(x_{ij})^{-1}] \cong k[x_{ij}, z]/(z \cdot \det(x_{ij}) - 1).$$

A *linear algebraic group* is a subgroup $G \subset \mathrm{GL}_m(k)$ which is closed in the Zariski topology. Then G is itself an affine variety with coordinate ring $k[G] = k[GL_m(k)]/I$, where I is the defining ideal of G. A finite dimensional representation $\rho : G \to \mathrm{GL}(V) \cong \mathrm{GL}_n(k)$ of a linear algebraic group G is called *rational* if ρ is also a morphism between affine varieties.

Example 3.1. $\mathrm{SL}_2(\mathbb{C}) \subset \mathrm{GL}_2(\mathbb{C})$ is the Zariski closed subset defined by the equation $\det = 1$. The representation of $\mathrm{SL}_2(\mathbb{C})$ on the space V of quadratic binary forms is given by

$$\rho : \mathrm{SL}_2(\mathbb{C}) \to \mathrm{GL}(V) \cong \mathrm{GL}_3(\mathbb{C}), \qquad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \to \begin{pmatrix} \alpha^2 & 2\alpha\gamma & \gamma^2 \\ \alpha\beta & \alpha\delta + \beta\gamma & \gamma\delta \\ \beta^2 & 2\beta\delta & \delta^2 \end{pmatrix}.$$

Thus ρ is a polynomial map, hence ρ is a rational representation. □

Definition 3.2. An algebraic group G is said to be *linearly reductive*, if every finite dimensional rational representation of G is *completely reducible*, that is, a direct sum of irreducible representations. □

Since we are interested in actions of groups on polynomial rings we must consider infinite dimensional representations as well. If G is linear algebraic, a representation of G on an arbitrary vector space over k is called *rational* if every vector is contained in a finite dimensional G–invariant subspace W such that the induced representation on W is rational in the sense above. The following is easy to prove (compare Springer (1989)).

Proposition 3.3. *Let G be a linear algebraic group. The following are equivalent:*

(1) G is linearly reductive.

(2) The defining condition in 3.2 holds for any rational representation of G.

(3) For any rational representation $\rho : V \to \mathrm{GL}(V)$ there exists a k-linear map $p_V : V \to V$, with $p_V \circ \rho(\pi) = p_V$ for all $\pi \in G$, which projects V onto the fixed point set $V^G = \{v \in V \mid \pi v = v \text{ for any } \pi \in G\}$.

(4) There exists an invariant integral *on G, that is, a map $I : k[G] \longrightarrow k$ with $I(1) = 1$ and $I \circ \lambda(\pi) = I$ for all $\pi \in G$, where λ is the representation of G on $k[G]$ given by $(\lambda(\pi)f)(\xi) = f(\pi^{-1}\xi)$.*

Remark 3.4. If a rational representation of a linearly reductive group G on a finite dimensional vector space V is given, then the third part of 3.3 applies in particular to the induced rational representation on $k[V]$. As is easy to see, the corresponding map $R : k[V] \to k[V]$ is in addition a $k[V]^G$–module homomorphism. R is called *Reynolds operator.*

Example 3.5.

(1) Let G be a finite group. Then G has the structure of a linear algebraic group with coordinate ring $k[G]$, where $k[G]$ is the k-algebra of k-valued functions on G with pointwise defined multiplication. Suppose that the

group order $|G|$ is invertible in k (*non-modular case*). Then G is linearly reductive (Maschke's theorem, see (Maschke 1899)). Indeed, if V is a rational representation of G then averaging over the group gives a map as in 3.3, (3).

$$V \to V, \quad v \to \frac{1}{|G|}\sum_{\pi \in G} \pi v.$$

(2) The multiplicative group k^* is a linear algebraic group with coordinate ring $k[z, z^{-1}]$. The map $\sum a_i z^i \mapsto a_0$ is an invariant integral. Therefore k^* is linearly reductive. More generally, every torus $(k^*)^m$ is linearly reductive.

(3) For linear algebraic groups which are compact in the $\mathbb{C}$–topology one can construct an invariant integral by integrating functions with respect to the Haar measure. This measure is obtained from an arbitrary measure by averaging over the group.

(4) A linear algebraic group G, which has a subgroup that is compact in the $\mathbb{C}$–topology and dense in the Zariski topology, is linearly reductive (see Kraft (1985)). The linear reductivity of the classical groups can be deduced from this fact. □

The Reynolds operator is abstractly defined, and in general it is not easy to get a hand on it. But in most situations it suffices that one is able to generate all invariants of a given degree. There are several ways for producing the invariants in a given degree, each adapted to a particular situation. We sketch the Lie algebra method and refer to Sturmfels (1993) for Cayley's Ω–process and the symbolic method. Consider a rational representation $\rho : G \longrightarrow \mathrm{GL}(W)$ of a linear algebraic group on a finite dimensional vector space W, and the induced action on the Lie-algebras:

$$\rho_* : \mathrm{Lie}(G) \longrightarrow \mathrm{Lie}(\mathrm{GL}(W)).$$

If $w \in W$ is G–invariant, then differentiating the expression $\pi w = w$ with respect to π, shows that $\phi w = 0$ for any element ϕ in $\mathrm{Lie}(G)$. The converse holds, as soon as G is *connected*. Applying this to $W = S^d(V^*)$ shows that one may find all invariants of a given degree by solving linear equations. If G is not connected, one should first find the invariants for the connected component G^0 of the identity, and then pick out those invariants of G^0 which are invariant under the finite group G/G^0.

We now give a proof of Hilbert's finiteness theorem (Hilbert 1890).

Theorem 3.6 (Hilbert's Finiteness Theorem). *Let G be a linearly reductive group, acting rationally on a finite dimensional vector space V. Then the ring of invariants $k[V]^G$ is finitely generated as a k–algebra.*

Proof. Consider the ideal $I_{\mathcal{N}}$ in $k[V]$ generated by the homogeneous invariants of positive degree. Hilbert's basis theorem implies that already finitely many of those generate $I_{\mathcal{N}}$:

$$I_{\mathcal{N}} = (f_1, \dots, f_r).$$

We claim that the invariants are generated as a k–algebra by $f_1, \dots, f_r$. If f is any homogeneous invariant of positive degree, then $f \in I$, so we can write $f = \sum h_i f_i$. Applying the Reynolds operator R yields:

$$f = \sum R(h_i) f_i.$$

The $R(h_i)$ are invariants, which we may assume to be of lower degree than f. By induction, the $R(h_i)$ are in the subalgebra generated by $f_1, \dots, f_r$. Hence so is f. $\square$

The proof, as it stands, is non–constructive, because one has to find generators of $I_{\mathcal{N}}$. Because of this, Hilbert was harshly criticized. (Gordan: "Das ist Theologie und keine Mathematik"). Let us quote from a letter of Minkowski to Hilbert from 1892 (see Minkowski (1973) and compare Derksen *et al.* (1995) for a translation into English):

(...) Dass es nur eine Frage der Zeit sein konnte, wann Du die alten Invariantenfragen soweit erledigt haben würdest, dass kaum noch das Tüpfelchem auf dem i fehlt, war mir eigentlich schon seit lange nicht zweifelhaft. Dass es aber damit so schnell geht, und alles so überraschend einfach gelingt, hat mich aufrichtig gefreut, und beglückwünsche ich Dich dazu. Jetzt, wo Du in Deinem letzten Satze sogar das rauchlose Pulver gefunden hast, nachdem schon Theorem I nur noch vor Gordans Augen Dampf gab, ist es wirklich an der Zeit, dass die Burgen der Raubritter STROH, GORDAN, STEPHANOS und wie sie alle heissen mögen, welche die einzelreisenden Invarianten überfielen und in's Burgverlies sperrten, dem Erdboden gleichgemacht werden, auf die Gefahr hin, dass aus diesen Ruinen niemals wieder neues Leben spriesst. (...)

Later on Gordan admitted, that "theology also has its advantages" (compare Kline (1972)). In particular, he gave a new proof of Hilbert's basis theorem (Gordan 1899). In today's language, this proof consists of two parts:

- Every ideal generated by monomials is finitely generated (Dickson's Lemma).
- Every ideal has a finite *Gröbner basis.*

Taking this historical discussion into account, it came with a big surprise that Derksen (1997) could refine the ideas of Hilbert (1890) and turn them into an algorithm. In fact, Derksen came up with an algorithm for finding homogeneous generators for the ideal $I_{\mathcal{N}}$ by using Gröbner bases. First he remarks that it easily follows from the above proof of Hilbert's finiteness theorem, that for any set of homogeneous generators $f_1, \ldots, f_r$ of $I_{\mathcal{N}}$, the ring of invariants is generated by $R(f_1), \ldots, R(f_r)$ (see Derksen (1997)). As usual, the Reynolds operator can be replaced by any other means of generating invariants of a given degree. To find generators of $I_{\mathcal{N}}$, Derksen considers the map

$$\psi : G \times V \longrightarrow V \times V, \qquad (\pi, v) \mapsto (v, \pi v).$$

Let B be the Zariski closure of the image of ψ, with defining ideal $J \subset k[V \times V] \simeq k[x, y]$. Here $y = y_1, \ldots, y_n$ is a new set of variables. Derksen proves that one can get generators for $I_{\mathcal{N}}$ by substituting $y = 0$ in a generating set of J, or to put it in another way:

Theorem 3.7.

$$((y) + J) \cap k[x] = I_{\mathcal{N}}.$$

Proof. " $\supset$ " Let $f(x) \in I_{\mathcal{N}}$ be an invariant of positive degree. Then $f(x) = f(y) + (f(x) - f(y)) \in ((y) + J)$ since $f(y)$ is in (y), and $(f(x) - f(y))$ is in J. Indeed, $(f(x) - f(y))(v, \pi v) = f(v) - f(\pi v) = 0$, as f is G–invariant.

" $\subset$ " To prove the other inclusion we look at the action of G on $V \times V$ given by $\pi(v, w) = (v, \pi w)$. The corresponding Reynolds operator

$$R_y : k[x, y] \longrightarrow k[y]^G[x]$$

has the following properties:

(1) R_y is $k[x]$-linear.

(2) $R_y(J) \subset J$. This is because B is G–invariant.

(3) The diagonal $\Delta \subset V \times V$ is a subset of B. Thus J is contained in the ideal of the diagonal, that is, in the kernel of $\phi : k[x, y] \to k[x], \quad p(x, y) \mapsto p(x, x)$.

(4) The restriction of R_y to $k[y]$ is the Reynolds operator for the given action of G on V, since this operator is uniquely determined by its properties as in 3.3.

Now take any homogeneous $f(x) = \sum c_i(x) f_i(y) + h(x, y) \in ((y) + J) \cap k[x]$, with $f_i(y) \in (y)$ homogeneous, and $h(x, y) \in J$. We have $R_y(h(x, y)) \in J$ by (2), hence $\phi(R_y(h(x, y)) = 0$ by (3). Therefore, by (1) and (4),

$$f(x) = \sum c_i(x) \phi(R_y(f_i(y))) = \sum c_i(x) R(f_i(x)).$$

The $R(f_i)$ are homogeneous invariants of positive degree. Hence $f \in I_{\mathcal{N}}$. $\square$

Generators of J can be found by elimination, that is, via Gröbner bases. We consider an example.

Example 3.8. We take the action of $G = \mathrm{SL}_2(\mathbb{C})$ on the three dimensional vector space V of quadratic binary forms as in Example 3.1. Consider

$$\Gamma = \{(\pi, v, \pi v) : \pi \in G, v \in V\} \subset G \times V \times V.$$

Then B is the closure of $p(\Gamma)$, where p is the projection onto $V \times V$. The ideal

$$I \subset k[\alpha, \beta, \gamma, \delta, x_1, x_2, x_3, y_1, y_2, y_3]$$

of Γ is given by $(\alpha\delta - \beta\gamma - 1, -y_1 + \alpha^2 x_1 + 2\alpha\gamma x_2 + \gamma^2 x_3, -y_2 + \alpha\beta x_1 + (\alpha\delta + \beta\gamma)x_2 + \gamma\delta x_3, -y_3 + \beta^2 x_1 + 2\beta\delta x_2 + \delta^2 x_3)$. We eliminate $\alpha, \beta, \gamma, \delta$ via Gröbner bases. The result is the principal ideal

$$(x_2^2 - x_1 x_3 - y_2^2 + y_1 y_3).$$

Now we plug in $y_1 = y_2 = y_3 = 0$ and conclude that the discriminant $x_2^2 - x_1 x_3$, which is already invariant, generates the ring of invariants. $\square$

Hilbert himself reacted to the criticism by writing a second paper (Hilbert 1893) in which he gave a constructive way of finding generators for the ring of invariants in the case of $\mathrm{SL}_n(\mathbb{C})$ acting on forms (or systems of forms) by linear substitution. Let us sketch this method. Instead of looking for generators of the ideal $I_{\mathcal{N}}$, Hilbert asks for homogeneous invariants cutting out the variety defined by $I_{\mathcal{N}}$. This variety is called the *Null-cone* by Hilbert. He first shows:

Theorem 3.9. *Let $f_1, \ldots, f_r$ be homogeneous invariants whose zero–set is the Null-cone. Then $K[V]^G$ is a finitely generated $K[f_1, \ldots, f_r]$-module.*

Proof. By the Nullstellensatz (proved in the same paper), there exists an $m > 0$, such that $I_{\mathcal{N}}^m \subset (f_1, \ldots, f_r)$. By applying the Reynolds operator and induction, it follows without too much difficulty that $k[V]^G$ is generated as a $K[f_1, \ldots, f_r]$–module by all invariants of degree $\leq mrd$. Here d is the maximum of the degrees of the f_i. $\square$

How to compute $f_1, \ldots, f_r$ as above? Consider the maximal torus T in G, and compute its ring of invariants $k[V]^T$ via integer programming, see (Sturmfels 1993, section 1.4). The zero-set of the torus invariants of positive degree is called the *canonical cone*. The Hilbert–Mumford criterion (Hilbert 1893, Mumford *et al* 1994), compare also Kraft (1985), says that the Null-cone is the orbit under G of the canonical cone. It follows that one can find $f_1, \ldots, f_r$ as above from the torus invariants via Gröbner bases (see Sturmfels (1993)).

At this point, Hilbert gives two alternatives how to proceed. We sketch the first method.

(1) Compute a Noether normalization $k[p_1, \ldots, p_m]$ of $k[f_1, \ldots, f_r]$. Then $k[p_1, \ldots, p_m] \subset k[V]^G$ is also a Noether normalization, and therefore every element of $k[V]^G$ is integral over $k[p_1, \ldots, p_m]$.

(2) Compute the *quotient field* of $k[V]^G$.

(3) Via the theorem of the primitive element, find a further invariant p such that $k(p_1, \dots, p_m, p)$ is equal to the quotient field of $k[V]^G$.

(4) It now follows easily that the *normalization* of $k[p_1, \dots, p_m, p]$ is equal to $k[V]^G$.

For Hilbert's second method, which also reduces the problem to the computation of a normalization, we refer to Sturmfels (1993).

An efficient algorithm for computing the normalization has been recently described by de Jong (1997). This algorithm is implemented in Singular (Decker *et al.* 1997). See Greuel *et al.* (1997) for Singular.

References

Adler, A. (1992) 'Invariants of the Simple Group of Order 660 acting on $\mathbb{C}^5$', *Comm. Alg.* **22**, 2837–2862.

Adler, A. (1997) 'Invariants of $\mathrm{SL}_2(\mathbb{F}_q) \cdot \mathrm{Aut}(\mathbb{F}_q)$ acting on $\mathbb{C}^n$', Preprint.

Bertin, M.–J. (1967) 'Anneaux d'invariants d'anneaux de polynomes en caractéristique p', *Comptes Rendus Acad. Sci. Paris (Serie A)* **264**, 653–656.

Bruns, W., Herzog, J. (1993) 'Cohen–Macaulay rings', Cambridge University Press, Cambridge.

Buchberger, B. (1965) 'On Finding a Vector Space Basis of the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal' (German). PhD Thesis, Univ of Innsbruck, Austria.

Buchberger, B. (1970) 'An Algorithmical Criterion for the Solvability of Algebraic Systems of Equations' (German), *Aequationes mathematicae* **4**, 374–383.

Buchberger, B. (1985) 'Gröbner-Bases: An Algorithmic Method in Polynomial Ideal Theory.' Chapter 6 in: Multidimensional Systems Theory (N.K. Bose ed.), Reidel Publishing Company, Dordrecht, 1985, 184-232.

Buchberger, B. (1998) 'Introduction to Gröbner Bases', this volume.

Campbell, H.E.A., Hughes, I.P., Pollack, R.D. (1991) 'Rings of Invariants and p-Sylow Subgroups', *Can. Math. Bull.* **34**, 42–47.

Cox, D., Little, J., O'Shea, D. (1997) 'Ideals, Varieties, and Algorithms, second ed.', Springer, New York.

Decker, W., Greuel, G.–M., de Jong, T., Pfister, G. (1997) 'The Normalization: a New Invented Algorithm, Implementation and Comparisons', Preprint, Kaiserslautern, Saarbrücken.

Decker, W., Heydtmann, A. E., Schreyer, F.-O. (1997) 'Generating a Noetherian Normalization of the Invariant Ring of a Finite Group', J. Symbolic Computation (to appear).

Derksen, H. (1997a) 'Constructive Invariant Theory and the Linearization Problem', Thesis, Basel.

Derksen, H. (1997b) 'Computation of Invariants for Reductive Groups', Preprint, Basel.

Derksen, H., Kraft, H. (1995) 'Constructive Invariant Theory', Preprint, Basel.

Dieudonné, J.A., Carrell, J.B. (1971) 'Invariant Theory, Old and New', Academic Press, New York, London.

Eisenbud, D. (1995) 'Commutative Algebra with a View Toward Algebraic Geometry', Springer, New York.

Eisenbud, D., Riemenschneider, O., Schreyer, F.-O. (1981) 'Projective Resolutions of Cohen-Macaulay Algebras', *Math. Ann.* **257**, 85–98.

Gauss, C.F. (1801) 'Disquisitiones arithmeticae', translation A.A. Clarke, Yale University Press, 1965.

Gianni, P., Trager, B. (1996) 'Integral Closure of Noetherian Rings', Preprint.

Gordan, P. (1868) 'Beweis, dass jede Covariante und Invariante einer binären Form eine ganze Funktion mit numerischen Coeffizienten einer endlichen Anzahl solcher Formen ist', *J. Reine Angew. Math.* **69**, 323–354.

Gordan, P. (1899) 'Neuer Beweis des Hilbertschen Satzes über homogene Funktionen', *Nachrichten König. Ges. der Wiss. zu Gött.*, 240–242.

Greuel, G.-M., Pfister, G., Schönemann, H. (1997) 'Singular Reference Manual', *Reports On Computer Algebra, number 12.* Centre for Computer Algebra, University of Kaiserslautern,
http://www.mathematik.uni-kl.de/~zca/Singular.

Heydtmann, A.E. (1996) 'Generating Invariant Rings of Finite Groups', Diplom Thesis, Saarbrücken.

Heydtmann, A.E. (1997) 'finvar.lib: A Singular Library to Compute Invariant Rings and more', http://www.mathematik.uni-kl.de/~zca/Singular.

Hilbert, D. (1890) 'Über die Theorie der algebraischen Formen', *Math. Ann.* **36**, 473–534.

Hilbert, D. (1893) 'Über die vollen Invariantensysteme', *Math. Ann.* **42**, 313–373.

Hilbert, D. (1900) 'Mathematische Probleme', *Nachr. v. d. Ges. d. Wiss. zu Göttingen*, 253–297.

Hochster, M., Eagon, J.A. (1971) 'Cohen–Macaulay Rings, Invariant Theory, and the Generic Perfection of Determinantal Loci', *Am. J. Math.* **93**, 1020–1058.

Hochster, M., Roberts, J. (1974) 'Rings of Invariants of Reductive Groups Acting on Regular Rings are Cohen-Macaulay', *Adv. in Math.* **13**, 115–175.

Horrocks, G., Mumford, D. (1973) 'A Rank 2 Vector Bundle on $\mathbb{P}^4$ with 15,000 Symmetries', *Topology* **12**, 63–81.

de Jong, T. (1997) 'An Algorithm for Computing the Integral Closure', Preprint, Saarbrücken.

Kemper, G. (1993) 'The Invar Package for Calculating Rings of Invariants', *IWR Preprint Universität Heidelberg*, 93-94.

Kemper, G. (1996) 'Calculating Invariant Rings of Finite Groups over Arbitrary Fields', *J. Symbolic Computation* **21**, 351–366.

Kemper, G. (1997) 'Calculating Optimal Homogeneous Systems of Parameters', *IWR Preprint Universität Heidelberg*, 97-08.

Kemper, G., Steel, A. (1997) 'Some Algorithms in Invariant Theory of Finite Groups', Preprint.

Klein, F. (1878/1879) 'Über die Transformationen siebenter Ordnung der elliptischen Funktionen', *Math. Ann.* **14**, 428–471.

Klein, F. (1879) 'Über die Transformationen elfter Ordnung der elliptischen Funktionen', *Math. Ann.* **15**, 533–555.

Kline, M. (1972) 'Mathematical Thought from Ancient to Modern Times', Oxford University Press, New York.

Kraft, H. (1985) 'Geometrische Methoden in der Invariantentheorie', Vieweg, Braunschweig.

Kung, J.P.S., Rota, G.–C. (1984) 'The Invariant Theory of Binary Forms', *Bull. Am. Math. Soc.* **10**, 27–85.

de Lagrange, J.–L. (1773, 1775) 'Recherches d'arithmétique', Œuvres, vol. 3, 695–795, Georg Olms Verlag, Hildesheim, New York 1973.

Maschke, H. (1899) 'Beweis des Satzes, dass diejenigen endlichen linearen Substitutionsgruppen, in welchen einige durchgehende verschwindende Coeffizienten auftreten, intransitiv sind', *Math. Ann.* **52**, 363–368.

Minkowski, H. (1973) ' Briefe an David Hilbert, mit Beiträgen und herausgegeben von L. Rüdenberg und H. Zassenhaus', Springer, Berlin, Heidelberg, New York.

Möbius, F. (1827) 'Der barycentrische Calcul', Gesammelte Werke, vol. 1, 1-388, Wiesbaden 1885.

Molien, T. (1897) 'Über die Invarianten der linearen Substitutionsgruppen', *Sitzungsber. König. Preuss. Akad. Wiss.*, 1152–1156.

Mumford, D., Fogarty, J., Kirwan, F. (1994) 'Geometric Invariant Theory', third ed., Springer, Berlin, Heidelberg, New York.

Newstead, P. (1978) 'Introduction to Moduli Problems and Orbit Spaces', Springer, Berlin, Heidelberg, New York.

Noether, E. (1916) 'Der Endlichkeitssatz der Invarianten endlicher Gruppen', *Math. Ann.* **77**, 89–92.

Noether, E. (1926) 'Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p', *Nachr. v. d. Ges. d. Wiss. zu Göttingen*, 28–35.

Plücker, J. (1830) 'Über ein neues Coordinatensystem', *J. Reine Angew. Math.* **5**, 1–36.

Schreyer, F.–O. (1980) 'Die Berechnung von Syzygien mit dem verallgemeinerten Weierstrass'schen Divisionssatz', Diplom Thesis, Hamburg.

Sloane, N.J.A. (1977) 'Error Correcting Codes and Invariant Theory: New Applications of a Nineteenth Century Technique', *Am. Math. Monthly* **84**, 82–107.

Smith, L. (1995) 'Polynomial Invariants of Finite Groups', A.K. Peters, Wellesley.

Springer, T.A. (1989) 'Aktionen reduktiver Gruppen auf Varietäten', Algebraische Transformationsgruppen und Invariantentheorie, DMV-Seminar Notes 13, Birkhäuser, Basel, Boston.

Stanley, R. B. (1979) 'Invariants of Finite Groups and their Applications to Combinatorics', *Bull. Am. Math. Soc.* **1**, 475–511.

Sturmfels, B. (1993) 'Algorithms in Invariant Theory', Springer, Wien, New York.

Sylvester, J.J. (1904–1912) 'The Collected Mathematical Papers of James Joseph Sylvester', Cambridge University Press, Cambridge.

Vasconcelos, W. (1991) 'Computing the Integral Closure of an Affine Domain', *Proc. AMS* **113**, 633–638.

Weyl, H. (1946) 'The Classical Groups, their Invariants and Representations', second ed., Princeton Mathematical Series 1, Princeton University Press, Princeton.